Attorney's Docket No.: 10559/383001 / P10189

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: DECRYPTION KEY MANAGEMENT IN REMOTE NODES

APPLICANT: DMITRII LOUKIANOV, HOWARD HARTE, AND JABE A. SANDBERG

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL688267855US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

November 29, 2000
Date of Deposit

M. E. Augustine
Signature

Mike Augustine
Typed or Printed Name of Person Signing Certificate

DECRYPTION KEY MANAGEMENT IN REMOTE NODES

BACKGROUND

DOCSIS cable modem networks may control access to data using security and encryption techniques.

A current way of operating a DOCSIS cable modem uses data encryption standard (DES) encryption to restrict cable modem users from accessing data which they are not authorized to access. Different kinds of network data may be restricted.

One class of cable modem network data that is often restricted is so-called "multicast" data. This is data that is transmitted to more than one cable modem. The multicast data should be made accessible to a given group of cable modems on the network. It must, however, remain inaccessible to those cable modems that are not in the group. By preventing access to the unauthorized cable modems, those unauthorized cable modems are prevented from stealing the data service.

The cable head end controls the access to the multicast data by transmitting DES decryption keys in a "unicast" mode. The keys are sent individually, and are sent to only those cable modems that request the access and are also authorized to access the specified data. The

decryption keys themselves may be encrypted using, for example, triple CES or some other algorithm.

Other applications may also exist for allowing certain cable modems to access data while preventing other cable modems from accessing the data.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects will now be described in detail with reference to the accompanying drawings, wherein:

Figure 1 shows a CCCM implementation of key extraction.

Figure 2 shows how key extraction in a host migrated cable modem may cause a security threat;

Figure 3 shows a MAC chip and its decryption key handling capabilities;

Figure 4 shows more detail of the arrangement of the key material register bank;

Figure 5 shows a flowchart of security measures;

Figure 6 shows this system being used for more generalized protection.

DETAILED DESCRIPTION

It is often considered to be an unacceptable security breach if an unauthorized cable modem can gain access to unauthorized data. For example, a breach would be established if the cable modem could receive and use a DES decryption key that is not intended for that specific cable modem.

A conventional cable modem achieves this security by modifying the hardware in a way that ensures this kind of security. The conventional cable modem only accepts unicast transmissions that are addressed to the specific cable modem. The hardware within the modem rejects all other unicast transmissions. The cable modem only accepts keys from cable unicast transmissions.

The cable modem is configured to reject keys that are from any other source, such as from the host computer. The cable modem is also prohibited from sending any key reading material outside the cable modem.

For example, the cable modem CPU (central processing unit)/and or MAC (media access controller) chips will extract and use the multicast key internally. The hardware is configured to prevent the keys from being sent outside the cable unit.

This security can be addressed easily in hardware for

a conventional cable modem in which many of the operations are carried out in hardware. However, this becomes more complicated in certain new cable modems called "host-migrated modems", or CPE controlled cable modems or CCCMs. In CCCMs, many of the functions of these modern cable modems are migrated to software that runs on the host computer.

Since parts of the functions of the cable modem runs in the host computer, the present inventors recognize the desirability of migrating key extraction to the host computer. Figure 1 shows a CCCM implementation of key extraction.

The cable modem 100 receives a message 105 which includes encrypted key reading material which is passed through the cable modem as 110 to the host PC 150. Driver software 155 running in the host PC receives the key ring material and a decryption software layer 160 decrypts the keyring material and returns that decrypted key ring material 165 to the cable modem 100.

A traffic decryption engine 115 running in the cable modem 100 receives the decrypted key ring material and uses that material 165 for decrypting certain data.

However, the host PC (personal computer) 150, in this situation, may obtain access to the key ring material.

Moreover, this action may pose a security violation, since this means that the host migrated cable modem must accept keys from an external source. The PC is an inherently insecure element, since the user has access to its operating system and operation techniques of the PC.

For example, as shown in figure 2, a modem 199 receives encrypted key ring material over its cable connection. This message with encrypted key ring material is sent to the host PC 210. A rogue software component 200 on PC 210 could intercept keys on that PC 210. Those keys could then be retransmitted at 220 to an unauthorized modem on another PC 230. The transmission can be via the existing cable channel ("in band") or over some other channel ("out of band") such as by telephone modem. That unauthorized modem 240 could then steal the service intended for the authorized modem 199.

The present application defines a host migrated cable modem with special key handling security which avoids this security issue.

The special security operates to only accept keys which are sent in a specified away. In one embodiment disclosed herein, the cable modem only accepts keys from cable unicast transmissions, and not from any other source.

In the specific cable modem described herein, a media

access controller (MAC) chip 300 is used to carry out parts of key management. The Mac chip 300 includes a key material register bank 305 and a DES decryption engine 310 as shown in figure 3. Both of these blocks 305 and 310 are implemented totally in hardware, thereby allowing them to be considered as secure. The key material register bank 305 stores a key set for each data service flow as identified by its service ID. The key material register bank is shown in more detail in figure 4. Each service ID 400 includes different storage areas which enable write enable, key destroy, and the actual key material.

In this system, a key can only be used and accepted by the DES decryption engine 310 after it has been successfully placed into the key material register bank 305 that is stored physically within the media access controller chip 300.

The key material register bank 305 also includes a write enable function 405 for each service ID, and a key destroy function 410 for each service ID.

In operation, various restrictions are imposed on acceptance and/or use of a key which is obtained from the host PC. This compares with previous systems which have allowed acceptance and use of any key at any time. The restrictions are implemented by the above-described write

enable and write disable, as well as key invalidation and/or destruction.

Rules for key management are also provided. The rules are illustrated in the flowchart of figure 5. According to this flowchart, the system starts up at 500 with all keys for all service IDs being disabled. This means that no service ID can write a key to the register until something changes after startup. This provides a first basis for key security.

Additional rules are also defined. A cable modem only receives messages on the cable that are addressed to the specific cable modem.

At 505, the system determines if a current message is addressed to the current cable modem. If not, the message is disregarded at 510. This provides a mechanism for the head end to securely address a particular cable modem at a particular time.

If the current message is properly addressed at 505, then 515 determines if the message contains key ring material. A message which does not contains key ring material is processed normally at 520. If the message does contain key ring material at 515, then another rule is executed, for the specific service ID. This enables writing of the key material, and using the key ring

material at legitimate times. Legitimacy can be determined by the network's existing security mechanisms.

At 520, the encrypted key ring material is passed to the host for decryption. At 525, write enable for the specific service ID within the material is enabled. This enables writing that decrypted key ring material from the host, to the key material register bank, for the specified service ID.

At 530, the decrypted key ring material is received. The buffer determines at 535 if key write is enabled for the specific ID. If not, then the key ring material is disregarded at 540. If key write has been enabled for the specified service ID at 535, then the key ring material is written at 545. As soon as key ring material is written, key write is disabled shown as 550. This limits key writing to legitimate times only.

An extra aspect may disable key write for some given length of time, regardless of other operations, after a first writing. This extra technique would be executed after 550 if desired. If the new service ID number has been written to the key storage register bank at 555, then key ring material for that service ID is destroyed at 560. Key write for that service ID is also disabled at 565. This protects the security system from a subversion of

receiving legitimate key messages that are intended for one lower value service ID, and then using the write enable opportunity to write key ring material for a different, e.g., higher value, service ID.

These rules do not prevent the keys from being obtained illicitly, but rather prevent those keys from being used in an unauthorized cable modem. The rogue key ring material can still be distributed. However, it cannot be used once distributed.

The DOCSIS cable modem key distribution scheme also permits use of authorization keys. These are derived key encryption keys. Similar techniques can be used to protect these other keys. However, by protecting keys which are transmitted in a unicast mode, all other keys and key techniques can be similarly protected.

While the above has described operation in a host migrated cable modem, this system can be used in other cable modems including non host migrated modems. This can increase the security on the cryptographic system, even though existing cable modems are already considered to be secure.

This system can also be used in other types of modems besides cable modems and can be used in any other type modem in which encryption keys may be transmitted. This

system can also be used in simple network management protocol (SNMP) where access to certain information or controls in the modem must be controlled. The SNMP messages may be delivered by insecure paths or methods, since these techniques prevent keys within the message from being used unless they meet the specified requirements.

This system may also have application beyond modems, i.e. to other type equipment that have remote control capabilities from a secure controller to one or a plurality of controlled nodes. Remote control commands issued by the secure controller must pass through insecure processing and/or channels before being received or applied by the equipment. This could include cable boxes or other set-top boxes, home gateways, industrial automation and/or telemetry equipment.

The generalized protection case is shown in figure 6. In this case, this same system is used to protect a more generalized system. A central controller 600 is shown controlling controlled nodes 605, 610. Each controlled node such as 605 includes an individual node controller 615. The node controllers are connected by a communication channel 620. This communication channel can be the Internet, a wireless channel, or any other form of communication between the noted controllers. Each node

controller is capable of receiving rogue software or commands 625. These are generically shown as security threats.

In this system, the same techniques are used as described above to securely detect remote control events, provide a remote control gating, and/or apply the contents from the processed messages only been enabled by the secure controller. After that control command, acceptance may be disabled.

Other modifications beyond those described herein are also possible. All such modifications are intended to be encompassed within the following claims.